Sum-free subsets of finite abelian groups of type III

R. Balasubramanian, Gyan Prakash and D.S. Ramana

Abstract

A finite abelian group G of order n is said to be of type III if all divisors of n are congruent to 1 modulo 3. We obtain a classification theorem for sum-free subsets of cardinality very "close" to the largest possible in a finite abelian group G of type III. This theorem, when taken together with known results, gives a complete characterisation of sum-free subsets of the largest cardinality in any finite abelian group G. We then give two applications of this theorem. Our first application allows us to write down a formula for the number of orbits under the natural action of $\mathrm{Aut}(G)$ on the set of sum-free subsets of G of the largest cardinality when G is of the form $(\mathbf{Z}/m\mathbf{Z})^r$, with all divisors of m congruent to 1 modulo 3, thereby extending a result of Rhemtulla and Street. Our second application provides an upper bound for the number of sum-free subsets of G. For finite abelian groups G of type III and with *a given exponent* this bound is substantially better than that implied by the bound for the number of sum-free subsets in an arbitrary finite abelian group, due to Green and Ruzsa.

1 Introduction

A subset A of an abelian group G is said to be *sum-free* if the sum of any pair of elements of A lies in the complement of A. In other words, A is sum-free if there is no solution to the equation $x + y = z$ with $x, y, z \in A$. For example, the subset of odd integers is a sum-free subset of the group $\mathbf{Z}$. By means of orthogonality of characters it is then easily seen that for a subset A of a finite group G to be sum-free it is necessary and sufficient that

$$\sum_{\gamma \in \widehat{G}} |\widehat{A}(\gamma)|^2 \widehat{A}(\gamma) = 0, \tag{1}$$

where $\widehat{G}$ is the group of characters on G and for any $\gamma \in \widehat{G}$, we have $\widehat{A}(\gamma) := \sum_{a \in A} \gamma(a)$ is the Fourier transform of the indicator function of the set A.

The study of sum-free subsets of abelian groups is the subject of a number of investigations in the literature, the most relevant to this article being the work [5] of Ben Green and Imre Ruzsa. For the purpose of studying their sum-free subsets, it is convenient to classify finite abelian groups into three *types* (see [5, Definition 1.4]). A finite abelian group G of order n is said to be of type III if all divisors of n are congruent to 1 modulo 3. The present article examines sum-free subsets in a finite abelian group of type III. In partcular, We study the question of obtaining a structure of sum-free subsets (Theorem 1.2) and also to give a count for the total number of sum-free sets (Theorems 1.6 and 1.7) in a finite abelian group of type III.

When G is not of type III, the largest possible cardinality $c(G)$ of a sum-free set in G was obtained by Diananda and Yap [2]. For a general G of type III, the value of $c(G)$ was obtained by Green and Ruzsa [5].

Theorem 1.1. *[5, Theorem 1.5] When G is a finite abelian group of exponent m and exponent n, the largest posible cardinality $c(G)$ of sum-free subset in G is equal to*

$$n\left(\max_{d|m}\frac{\left[\frac{d-2}{3}\right]+1}{d}\right). \tag{2}$$

The main result of the first part of this article is a classification theorem , Theorem 1.2 below, which characterises sum-free subsets with cardinality $c(G)$, when G is a finite abelian group of type III.

Let us recall that when G is an abelian group, the *supplement* H in G of a subgroup M of G is a subgroup of G such that the canonical map $(x, y) \to x+y$ from $H \oplus M$ into G is an isomorphism. When G is a finite abelian group of exponent m, every subgroup of G isomorphic to $\mathbf{Z}/m\mathbf{Z}$ has a supplement in G. A *splitting* of G by $\mathbf{Z}/m\mathbf{Z}$ is a pair (H, f) where f is an injective homomorphism from $\mathbb{Z}/m\mathbb{Z}$ into G and H is a supplement of the image of f in G. When (H, f) is a splitting of G by $\mathbf{Z}/m\mathbf{Z}$ and B, C are, respectively, subsets of H and $\mathbf{Z}/m\mathbf{Z}$, we write $(B, C)_{(H,f)}$, or simply (B, C), to denote the subset $B + f(C)$ of G. Moreover given any element $x_1 \in H, x_2 \in \mathbb{Z}/m\mathbb{Z}$, we write (x_1, x_2) to denote the element $x_1 + f(x_2)$ in G. It follows from definitions that given any element $x \in G$, there exists unique element (x_1, x_2) with $x_1 \in H$ and $x_2 \in \mathbb{Z}/m\mathbb{Z}$ such that $x = (x_1, x_2)$.

When X is a subset of $\mathbf{Z}$, and m an integer we write X_m to denote the canonical image of X in $\mathbf{Z}/m\mathbf{Z}$. For example, suppose that a and b are integers with $a < b$. We then write $[a, b]_m$ to denote the canonical image in $\mathbf{Z}/m\mathbf{Z}$ of the set of integers in the interval $[a, b]$.

Finally, let us note that since every divisor of a finite abelian group G of type III is congruent to 1 modulo 3, the exponent m of G is congruent to 1 modulo 6.

Theorem 1.2. *Suppose that G is a finite abelian group of type III and exponent m and let $k = \frac{m-1}{6}$. Let (H, f) be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$ and let K be a subgroup of H and K^c denote the complement of K in H. Then each of the following is a sum-free subset of G of the largest possible cardinality.*

(i) $(H, [2k+1, 4k]_m)$.
(ii) $(K, \{2k\}_m) \cup (K^c, \{4k\}_m) \cup (H, [2k+1, 4k-1]_m)$.
(iii) $(K, \{2k\}_m) \cup (K, \{4k+1\}_m) \cup (K^c, \{4k\}_m) \cup (K^c, \{2k+1\}_m) \cup (H, [2k+2, 4k-1]_m)$.

Every sum-free subset of G of the largest possible cardinality is one of the above for some splitting of G by $\mathbb{Z}/m\mathbb{Z}$.

Definition 1.3. Let G be a finite abelian group of type III. Given a splitting (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$ and a subgroup K of H, we shall write $L(H, f, 0), L(H, f, K, I), L(H, f, K, II)$ to denote the sets as in (i), (ii), (iii) of Theorem 1.2, respectively. If $L \subset G$ is equal to one of this sets then we say that L has a *presentation* with respect to (H, f).

To the extent we are aware, Theorem 1.2 was formerly known only for groups of the form $(\mathbf{Z}/p\mathbf{Z})^r$, due to Rhemtulla and Street [8], and in a small number of additional cases. Moreover, when this theorem is read together with the results of Diananda and Yap [2], one obtains a complete characterisation of sum-free subsets of the largest cardinality in all (three) types of finite abelian groups.

Let A be a set from (i), (ii), or (iii) of Theorem 1.2. The first claim of Theorem 1.2 is that A is a sum-free subset of the largest possible cardinality in G. That A is sum-free follows on noting that, given elements $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in G$ with $(x_1, x_2) + (y_1, y_2) = (z_1, z_2)$, we must have $x_1 + y_1 = z_1$ and $x_2 + y_2 = z_2$. It is also easy to verify that $\mathrm{card}(A) = \frac{2kn}{m}$ which from Theorem 1.1 is equal to the maximum possible cardinality of a sum-free subset of G.

We supplement Theorem 1.1 with the following result, which allows access to the structure of sum-free subsets of G of cardinality "close" to the largest possible in G.

Theorem 1.4. *Let G be a finite abelian group of type III of exponent m and cardinality n. When A is a sum-free subset of G with $\mathrm{Card}(A) = c(G) - \epsilon n$, where $\epsilon < \min(\frac{1}{6m}, 10^{-23})$, there exists a sum-free subset L of the largest possible cardinality $c(G)$ in G such that $\mathrm{Card}(A \setminus L) \leq 4\epsilon n$.*

The conclusion of Theorem 1.4 is "essentially" best possible. Indeed, there are examples of sum-free sets A satisfying the assumptions of Theorem 1.4 such that there does not exists any sum-free set L of the largest possible cardinality in G with $\mathrm{Card}(A \setminus L) \leq 2\epsilon n$.

In the second part of this article, comprising Sections 6 and 7, we detail our first application of Theorem 1.2. More precisely, when G is a finite abelian group, let $\mathrm{Aut}(G)$ and $\mathcal{L}(G)$ denote, respectively, the group of automorphisms of G and the set of all sum-free subsets of the largest possible cardinality in G. Given any $A \in \mathcal{L}(G)$ and $f \in \mathrm{Aut}(G)$, we have $f(A) \in \mathcal{L}(G)$. This defines a natural action of $\mathrm{Aut}(G)$ on $\mathcal{L}(G)$. Let H be a supplement of a copy of $\mathbb{Z}/m\mathbb{Z}$ in G and $\mathcal{R}(H)$ be the set of subgroups of H. Given $K \in \mathcal{R}(H)$ and $f \in \mathrm{Aut}(H)$, we have $f(K) \in \mathcal{R}(H)$. This defines an action of $\mathrm{Aut}(H)$ on $\mathcal{R}(H)$. With the aid of the classification theorem we deduce fairly easily that the problem of computing the number of orbits of $\mathcal{L}(G)$ under the action of $\mathrm{Aut}(G)$, when G is of type III, is equivalent to the problem of counting the number of orbits of $\mathcal{R}(H)$ under the action of $\mathrm{Aut}(H)$. More precisely, we obtain the following result.

Theorem 1.5. *When G is a finite abelian group of type III whose cardinality is n and exponent m, we have the relation*

$$\mathrm{Card}(\mathcal{L}(G)/\mathrm{Aut}(G)) = 2\mathrm{Card}(\mathcal{R}(H)/\mathrm{Aut}(H)) + \epsilon, \tag{3}$$

where ϵ is 0 when $m = 7$ and 1 otherwise.

This conclusion allows us to verify Theorem 1.6 below, which generalises a result of Rhemtulla and Street [8], who obtained it for the groups $(\mathbf{Z}/p\mathbf{Z})^r$, where p is a prime number congruent to 1 modulo 3.

Theorem 1.6. *When m is an integer with every divisor of m being congruent to 1 modulo 3, the number of orbits under the action of the group of automorphisms of $(\mathbf{Z}/m\mathbf{Z})^{r+1}$ on the set of sum-free subsets of the largest cardinality in $(\mathbf{Z}/m\mathbf{Z})^{r+1}$ is*

$$2\prod_{p|m} \binom{v_p(m) + r}{r} \; + \; \epsilon(m) \; , \tag{4}$$

where $v_p(m)$ is the exponent of the prime p in the decomposition of m into primes and $\epsilon(m)$ is 0 when m is 7 and is 1 otherwise.

Every subset of a sum-free subset is sum-free. Therefore we have that Card(SF(G)), where SF(G) denotes the set of all sum-free subsets of G, is at least $2^{c(G)}$, where $c(G)$ is the cardinality of a sum-free subset of the largest cardinality in G. A method for counting sum-free sets was developed by Green and Ruzsa in a series of papers. In [5, Theorem 1.9] they obtained an asymptotic formula for Card(SF(G)) in the case when the order of G is divisible by a small prime divisor of the form $3k+2$. However, obtaining an asymptotic formula for Card(SF(G)) appears to be a rather difficult problem when G is of type III, even in the special case when G is $(\mathbf{Z}/7\mathbf{Z})^r$. What is known are upper and lower bounds for Card(SF(G)) in terms of $2^{c(G)}$.

Indeed, Green and Ruzsa show in [5] that when G is $(\mathbf{Z}/7\mathbf{Z})^r$, we have the lower bound $\mathrm{Card}(\mathrm{SF}(G)) \geq 2^{c(G)+c(\ln n)^2}$, where $n = 7^r$ is Card(G). The same argument may be used to show a similar lower bound for any G of type III. On the other hand, for an upper bound we only have $\mathrm{Card}(\mathrm{SF}(G)) \leq 2^{c(G)+\frac{cn}{(\ln n)^{1/45}}}$, due to Green and Ruzsa, which may be improved to $\mathrm{Card}(\mathrm{SF}(G)) \leq 2^{c(G)+\frac{cn}{(\ln n)^{1/27}}}$, as observed by Balasubramanian and Gyan Prakash in [1]. These upper bounds are, however, valid in any finite abelian group G, not necessarily of type III.

In the third and final part of this article, comprising Sections 8 and 9, we apply the classification theorem to deduce the following result.

Theorem 1.7. *When G is a finite abelian group of type III whose cardinality is n and exponent m, the number of sum-free subsets of G does not exceed $2^{c(G)+c_m\, n^{2/3}(\log n)^{4/3}}$, where $c(G)$ is the cardinality of a sum-free subset of G of the largest cardinality and c_m depends only on m.*

In order to deduce the above theorem, we first apply the classification theorem to obtain an apparently novel relation between the number of subsets with prescribed doubling in H, where, as before H is a supplement of $\mathbf{Z}/m\mathbf{Z}$ in G, and the number of sum-free subsets of G. More precisely, for any positive integers t, k_1, k_2, and H any finite abelian group, we write $S(t, k_1, k_2, H)$ to denote the number of subsets B of H with $\mathrm{Card}(B) = k_1$ and $\mathrm{Card}(tB) = k_2$ and set

$$a(t, H) \;=\; \sum_{k_1,k_2\geq 1} \frac{S(t, k_1, k_2, H)}{2^{k_2}} \,. \tag{5}$$

When $t = 2$, we shall just write $S(k_1, k_2, H)$ and $a(H)$ to denote $S(2, k_1, k_2, H)$ and $a(2, H)$ respectively.

With this notation we have the following theorem.

Theorem 1.8. *When G is a finite abelian group of type III whose cardinality is n and exponent m, and H is a complement of $\mathbf{Z}/m\mathbf{Z}$ in G, we have the following relation.*

$$a(H)2^{c(G)} \leq \mathrm{Card}(\mathrm{SF}(G)) \leq n^2(a(H))^2 2^{c(G)} + o_m(2^{c(G)}) \,. \tag{6}$$

Ben Green has obtained an upper bound for $\mathrm{card}(S(k_1, k_2, H))$ in [3] when H is of the form $(\mathbf{Z}/p\mathbf{Z})^r$. Using a modification of his arguments, an upper bound for $\mathrm{card}(S(k_1, k_2, H))$ was obtained in [7], when H is an arbitrary finite abelian group. From this general bound and Theorem 1.8, we deduce Theorem 1.7.

Readers familiar with the work of Green and Ruzsa will recognise that our methods follow those of [5] closely. We conclude this introduction by acknowledging our debt to these authors.

2 A Sketch of Proof of Theorems 1.2 and 1.4.

Let us summarise the proofs of Theorems 1.2 and 1.4. The principle is to obtain these results from with the aid of the following proposition and Kneser's theorem.

Proposition 2.1. *Let G be a finite abelian group of type III, order n and exponent m. Let A be a sum-free subset of G with $\mathrm{card}(A) = c(G) - \epsilon n$ with $\epsilon \leq \min(10^{-23}, \frac{1}{6m})$. Then there exists a surjective homomorphism $f' : G \to \mathbb{Z}/m\mathbb{Z}$ such that*

$$A \subset f'^{-1}[2k, 4k+1]_m, \tag{7}$$

where $k = \frac{m-1}{6}$. In other words there is a splitting (H, f'') of G by $\mathbb{Z}/m\mathbb{Z}$ such that $H = \ker(f')$ and

$$A \subset (H, [2k, 4k+1]_m). \tag{8}$$

To prove Proposition 2.1 we shall use the following result of Green and Ruzsa.

Proposition 2.2. *[5, Propostion 7.2] Let G be a finite abelian group of type III and of order n. Then given any sum-free subset A of G with $\mathrm{card}(A) = c(G) - \epsilon n$, with $\epsilon \leq 10^{-23}$, there exists a surjective homomorphism $f : G \to \mathbb{Z}/q\mathbb{Z}$ with $q \neq 1$ such that*

$$A \subset f^{-1}[k+1, 5k]_q, \tag{9}$$

where $k = \frac{q-1}{6}$.

We provide a brief descriptiion of the arguments used in deducing Proposition 2.1 from Proposition 2.2. Let A be as in Proposition 2.1 and $f : G \to \mathbb{Z}/q\mathbb{Z}$ be a surjective homomorphism as given by Proposition 2.2. Using the arguments from [5] and the assumed lower bound for the cardinality of A it is easily seen that we have $q = m$. To verify that the assertion (9) may be strengthened to (7), we define a set $C(A) \subset \mathbb{Z}/m\mathbb{Z}$ as follows:

$$C(A) = \{i \in \mathbb{Z}/m\mathbb{Z} : \mathrm{card}(A \cap f^{-1}\{i\}) > \frac{n}{2m}\}.$$

From the pigeonhole principle we deduce that $C(A)$ is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$. An application of Kneser's theorem then shows that $\mathrm{card}(C(A)) = 2k$; that is, in fact $C(A)$ is a sum-free subset of the largest possible cardinality in $\mathbb{Z}/m\mathbb{Z}$. The structure of $C(A)$ is obtained by proving Theorem 1.2 in the case when G is cyclic. Using this we complete the proof of Proposition 2.1.

3 Preliminaries

The notation described in this section will be used throughout this article; we will, in addition, introduce other notations whenever required.

2.1 Notation in Abelian Groups.— We generally use G to denote a finite abelian group. We use A,B, C, ... to denote subsets of G and use H,H', K, K' for its subgroups. The group law in G will be written additively with 0 for the identity element of G. Further, n will denote the cardinality of G and m its exponent. When A and B are subsets of G, $A+B$ will denote the subset of G the image of the map $(x, y) \to x+y$ from $A \times B$ into G. A pair of subgroups (H, H') of G will be called *supplementary* if the map $(x, y) \to x + y$ from $H \oplus H'$ into G is an isomorphism.

2.2 Subsets of $\mathbf{Z}$. — We use the usual notation for intervals in $\mathbf{R}$ to mean the set of integers contained in these intervals. When X is a subset of the $\mathbf{Z}$ and $d \geq 1$ is an integer, X_d will denote the canonical image in $\mathbf{Z}/d\mathbf{Z}$ of the set X. For example, when a and b are real numbers with $a < b$ and m an integer ≥ 1, $[a, b)$ denotes the set of integers in the real interval $[a, b)$ and $[a, b)_d$ denotes the canonical image of this set in $\mathbf{Z}/d\mathbf{Z}$.

2.3 Elementary Properties of Sum-free Subsets.— Every subset of a sum-free subset of G is a sum-free subset of G. The inverse image of a sum-free subset of G under a homomorphism from G' to G is a sum-free subset of G'.

2.4 Density .— When G is a finite abelian group and A is a subset of G we write $\mu_G(A)$ to denote Card(A)/Card(G). We call $\mu_G(A)$ the *density* of A. When f is a surjective homomorphism of groups from G onto G', we have the relation $\mu_G(f^{-1}(A')) = \mu_{G'}(A')$ for every subset A' of G'. For each integer $d \geq 1$, we write μ_d to denote $\mu_{\mathbf{Z}/d\mathbf{Z}}([d/3, 2d/3)_d)$. It is easily verified that

$$\mu_d = \frac{\left[\frac{d-2}{3}\right] + 1}{d} \ . \tag{10}$$

2.6 Density of Sum-free Subsets of the Largest Cardinality. — When G is a finite abelian group we write $c(G)$ to denote the cardinality of any sum-free subset of largest cardinality in G and write $\mu(G)$ to denote $c(G)/\mathrm{Card}(G)$. If m is the exponent of G, then for each divisor d of m, $\mathbf{Z}/d\mathbf{Z}$ is a quotient of G. It follows from the above that for every divisor d of m, G contains a sum-free subset A_d for which $\mu_G(A_d) = \mu_d$. Consequently, $\mu(G) \geq \sup_{d|m} \mu_d$. From Theorem 1.1, we have that this inequality is in fact an equality.

2.7 Types of Abelian Groups. — A finite abelian group G is said to be of type I if there exists a prime divisor of n which is congruent to 2 modulo 3. When G is of type I and if p is the least among the primes congruent to 2 modulo 3 dividing n, we say that G is of type I(p). We say G is of type II if G is not of type I and if n is divisible by 3. Finally, G is said to be of type III if it is neither of type I nor of type II . Thus G is type III if and only if *all* divisors of n are congruent to 1 modulo 3. With this division into three types, the formula (2) gives the following explicit relations for $\mu(G)$.

$$\mu(G) = \begin{cases} \frac{1}{3} + \frac{1}{3p} \text{ when } G \text{ is of type I}(p), \\ \frac{1}{3} \text{ when } G \text{ is of type II}, \\ \frac{1}{3} - \frac{1}{3m} \text{ when } G \text{ is of type III}. \end{cases} \tag{11}$$

2.8 A Consequence of pigeon hole principle.—- We shall require the following lemma, which is an easy consequence of pigeon hole principle.

Lemma 3.1. *Let G be a finite group and H be its subgroup. For some $x, y \in G$, let A and B are subsets of G with $A \subset H + x$ and $B \subset H + y$. If* $\min(\mathrm{card}(A), \mathrm{card}(B)) > \frac{\mathrm{card}(H)}{2}$, *then $A + B = H + x + y$.*

2.9 A Consequence of Kneser's Theorem. — Let G be a finite abelian group acting on the set of its subsets by translation. For any $A \subset G$, we write $S(A)$ to denote the stabiliser of A in G. When B and C are subsets of G such that $\mathrm{Card}(B + C)$ does not exceed $\mathrm{Card}(B) + \mathrm{Card}(C) - 1$, we have by Kneser's theorem that

$$\mathrm{Card}(B + C) = \mathrm{Card}(B + H) + \mathrm{Card}(C + H) - \mathrm{Card}(H) \ , \tag{12}$$

where $H = S(B + C)$. As a consequence we easily deduce the following Lemma.

Lemma 3.2. *Let G be a finite abelian and $B \subset G$ with* $\mathrm{Card}(B+B) < \frac{3}{2}\mathrm{Card}(B)$. *Then $B+B$ is equal to a coset of $S(B+B)$ and consequently $B \subset S(B+B)+x$ for some $x \in G$.*

2.10 Schur Triples. — When G is a finite abelian group of order n and B is a subset of G, an element (x,y,z) of $B \times B \times B$ such that $x+y=z$ is called a *Schur triple*. We say that B is an *almost sum-free* subset of G if the number of Schur triples in $B \times B \times B$ is $o(n^2)$. The following results on almost sum-free subsets, due to Green and Ruzsa, will be crucial to our proof of the upper bound for $\mathrm{SF}(G)$ given by Theorem 1.7.

Theorem 3.3. *[4, Theorem 1.5] Let G be a finite abelian group. Then every almost sum-free subset of G may be written as $A \cup B$, where A is sum-free and* $\mathrm{Card}(B)$ *is $o(n)$.*

Theorem 3.4. *[5, Proposition 2.1'] When the cardinality n of a finite abelian group G is sufficiently large, there is a family $\mathcal{F}$ of subsets of G satisfying the following conditions.*
(i) Every sum-free subset of G is contained in some element of the family $\mathcal{F}$.
(ii) There are no more than $2^{n(\log n)^{-1/18}}$ subsets of G in $\mathcal{F}$.
(iii) Every element of $\mathcal{F}$ is almost sum-free. In fact, $\mathcal{F}$ can be chosen so that the number of Schur triples in any element of $\mathcal{F}$ does not exceed $n^2/(\log n)^{1/10}$.

2.11 Sets with small sumset. — Given a subset B of an abelian group H, positive inetegers k_1, k_2 recall that we write

$$S(k_1,k_2,H) = \mathrm{Card}\left(\{B \subset H : \mathrm{card}(B)=k_1, \mathrm{card}(B+B)=k_2\}\right)$$

and

$$a(H) = \sum_{k_1,k_2} \frac{S(k_1,k_2,H)}{2^{k_2}}.$$

When H is a vector space over a finite field $\mathbb{Z}/p\mathbb{Z}$, Ben Green has obtained an upper bound for the cardinality of $S(k_1,k_2,H)$ in [3, Proposition 26]. In [7], using a modification of the arguments of Green, the second author obtained an upper bound for $\mathrm{card}(S(k_1,k_2,H))$ for an arbitrary finite abelian group H and proved the following result.

Theorem 3.5. *[7, Theorem 6] Let H be a finite abelian group of order n. Then the cardinality of $S(k_1,k_2,H)$ is at most*

$$n^{\frac{4k_2\log_2 k_1}{k_1}} \min(k_1^{c\omega(n)(k_1k_2\log k_1)^{1/3}}\binom{k_2}{k_1-1}(k_1^3+1), k_1^{4k_1}),$$

where $\omega(n)$ denotes the number of distinct prime divisors of n and c is a positive absolute constant.

We shall also require the following result from [5].

Lemma 3.6. *[5, Lemma 7.3 (ii)] Let G be a finite abelian group of type III and $f : G \to \mathbb{Z}/q\mathbb{Z}$ be a homomorphism. Then for any sum-free subset A of G and $i \in \mathbb{Z}/q\mathbb{Z}$, we have* $\mathrm{card}(A_i) + \mathrm{card}(A_{2i}) \le \frac{n}{q}$, *where $A_i = f^{-1}\{i\} \cap A$.*

Proof. Since A is sum-free, the set $A_i + A_i$ is disjoint from the set A_{2i}. Hence we have

$$\mathrm{card}(A_{2i}) \le \frac{n}{q} - \mathrm{card}(A_i + A_i) \le \frac{n}{q} - \mathrm{card}(A_i).$$

Hence the lemma follows. □

4 Proof of Proposition 2.1

Let A be as given in Proposition 2.1. Then from Proposition 2.2 there exists a positive integer $q \neq 1$ and a surjective homomorphism $f : G \to \mathbb{Z}/q\mathbb{Z}$ such that

$$A \subset f^{-1}([k+1, 5k]_q),$$

where $k = \frac{q-1}{6}$. We shall first observe that q is equal to the exponent m of G.

For any $i \in \mathbb{Z}/q\mathbb{Z}$, we write A_i to denote the set $A \cap f^{-1}\{i\}$ and α_i to denote the number $\frac{\mathrm{card}(A_i)q}{n}$. We write I to denote the set $[k+1, 5k]_q$ and I_0 to denote the set $[2k+1, 4k]_q$. The following lemma was used in [5] and is easy to check.

Lemma 4.1. *The set I may be divided into $2k$ disjoint pairs of elements of the form $(y, y/2)$, with $y \in I_0$.*

Since $A \subset f^{-1}(I)$, using Lemma 4.1 we have

$$\mu_G(A) = \frac{1}{q} \sum_{i \in \mathbb{Z}/m\mathbb{Z}} \alpha_i = \frac{1}{q} \sum_{i \in I_0} \left(\alpha_i + \alpha_{i/2}\right). \tag{13}$$

The argument used to prove the following lemma are identical to that in [5] to deduce Theorem 1.1 from Proposition 2.2 for type III groups.

Lemma 4.2. *With the notations as above $q = m$.*

Proof. Using (13) and Lemma 3.6, we obtain that $\mu_G(A) \leq \frac{2k}{q} = \frac{1}{3} - \frac{1}{3q}$. Suppose the lemma is not true. In that case, since G is a type III group and q divides m, we have $q \leq \frac{m}{7}$. Therefore we obtain that $\mu_G(A) \leq \frac{1}{3} - \frac{7}{3m} \leq \mu(G) - \frac{2}{m}$. This is contrary to the assumed lower bound of $\mu_G(A)$. Hence we have $q = m$. □

4.1 Reduction to cyclic case

Given a set $A \subset G$ as in Proposition 2.1, we define $C(A)$ to be the subset of the *cyclic group* $\mathbb{Z}/m\mathbb{Z}$ as follows:

$$C(A) = \{i \in \mathbb{Z}/m\mathbb{Z} : \alpha_i > \frac{1}{2}\}. \tag{14}$$

In this subsection we shall prove Proposition 4.6 stated below, which shows that $C(A)$ is a sum-free subset of the largest cardinality in $\mathbb{Z}/m\mathbb{Z}$.

Lemma 4.3. *For any $i, j \in C(A)$, we have $\alpha_{i+j} = 0$; in particular $C(A)$ is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Given any $i, j \in C(A)$, using Lemma 3.1 with $H = \ker(f)$ we obtain that $A_i + A_j = f^{-1}\{i+j\}$. Since A is sum-free, the sets $A_i + A_j$ and A_{i+j} are disjoint. Hence the lemma follows. □

Lemma 4.4. *For any $i_0 \in [2k+1, 4k]_m$ we have $\alpha_{i_0} + \alpha_{i_0/2} \geq 1 - (\mu(G) - \mu_G(A))\, m$.*

Proof. Since $A \subset f^{-1}(I)$, using (13) we have

$$\mu_G(A) \leq \frac{1}{m} \sum_{i \in I_0, i \neq i_0} (\alpha_i + \alpha_{i/2}) + \frac{1}{m}(\alpha_{i_0} + \alpha_{i_0/2}).$$

Now using Lemma 3.6 we have that the first term in the right hand side of the above inequality is at most $\frac{2k-1}{m} = \mu(G) - \frac{1}{m}$. Thus the result follows. □

Lemma 4.5. *For any $i_0 \in [2k+1, 4k]_m$, exactly one element from the pair of elements $(i_0, \frac{i_0}{2})$ belongs to $C(A)$.*

Proof. From Lemma 4.3, $C(A)$ is sum-free. Therefore it can contain at most element from the pair $(i_0, 2i_0)$. Suppose the lemma is not true for some i_0. For consiceness of notation, let $i = i_0/2$. Using Lemma 4.4, we obtain that

$$\mathrm{Card}(A_i) + \mathrm{Card}(A_{2i}) > \frac{5n}{6m}. \tag{15}$$

Since neither i nor $2i$ is in $C(A)$, we obtain that

$$\min(\mathrm{card}(A_i), \mathrm{card}(A_{2i})) > \frac{n}{3m}.$$

Using the fact that the sets $A_i + A_i$ and A_{2i} are disjoint subsets of $f^{-1}\{2i\}$ and (15), we also obtain that

$$\mathrm{Card}(A_i + A_i) \leq \frac{n}{m} - \mathrm{Card}(A_{2i}) < \frac{n}{m} - (\frac{5n}{6m} - \mathrm{card}(A_i)) \leq \frac{3}{2}\,\mathrm{card}(A_i).$$

Therefore applying Lemma 3.2 with $\mathcal{B} = \mathcal{C} = A_i$, we obtain that $A_i + A_i = S(A_i + A_i) + g$, where $S(A_i + A_i)$ is the stabiliser of $A_i + A_i$ in G and $g \in G$. Therefore we obtain that

$$\mathrm{Card}(S(A_i + A_i)) = \mathrm{Card}(A_i + A_i) \geq \mathrm{Card}(A_i) > \frac{n}{3m}.$$

We also have $S(A_i + A_i)$ is a subgroup of G contained in H with $H = \ker(f)$. Since H is a type III group, any proper subgroup of H will have cardinality at most $\frac{n}{7m}$. Hence we obtain that $S(A_i + A_i) = H$ and $A_i + A_i = f^{-1}\{2i\}$. This implies that $A_{2i} = \emptyset$, which is contrary to our earlier conclusion that $\mathrm{card}(A_{2i}) > \frac{n}{3m}$, thus proving the lemma follows. □

Combining Lemmas 4.3 and 4.5, we obtain the following result.

Proposition 4.6. *The set $C(A)$ is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$ with $\mathrm{card}(C(A)) = 2k$; in other words, $C(A)$ is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$ of the largest possible cardinality. Further for any $i, j \in C(A)$, we have $\alpha_{i+j} = 0$.*

Remark 4.7. We note that Lemma 4.5 also follows by appealing to [5, Lemma 7.3 (iii)]. We have preferred to give a self contained proof.

4.2 Classification of sum-free subset of the largest cardinality in cyclic group.

In this section, we prove Theorem 1.2 in case $G = \mathbb{Z}/m\mathbb{Z}$. In particular, this gives the structure of $C(A)$, when A is a subset of general finite abelian group.

Let E be a sum-free subset of the largest cardinality in $\mathbb{Z}/m\mathbb{Z}$. From Proposition 2.2 and Lemma 4.2, it follows that $d.E \subset I = [k+1, 5k]_m$ for some $d \in (\mathbb{Z}/m\mathbb{Z})^*$, where $k = \frac{m-1}{6}$. Replacing E by $d.E$, we may assume that $E \subset I$.

We write E^c to denote the complement of E in $\mathbb{Z}/m\mathbb{Z}$. For any subset B of $\mathbb{Z}/m\mathbb{Z}$ and an element $x \in \mathbb{Z}/m\mathbb{Z}$, we write $\widetilde{B}$ and $\widetilde{x}$ respectively to denote their images in $\mathbb{Z}$ under the natural unfolding map from $\mathbb{Z}/m\mathbb{Z}$ to the interval $[0, m-1]$ in $\mathbb{Z}$. We write I_{-1}, I_0, I_1 to denote, respectively, the subsets $[k+1, 2k]_m$, $[2k+1, 4k]_m$ and $[4k+1, 5k]_m$

of $\mathbb{Z}/m\mathbb{Z}$. For any subset $B \subset \mathbb{Z}/m\mathbb{Z}$, we write $B_{-1}, B_0, B_1, \widetilde{B}_{-1}, \widetilde{B}_0, \widetilde{B}_1$ to denote the sets $B \cap I_{-1}, B \cap I_0, B \cap I_1, \widetilde{B} \cap \widetilde{I_{-1}}, \widetilde{B} \cap \widetilde{I}_0, \widetilde{B} \cap \widetilde{I}_1$, respectively.

The following lemma is an easy consequence of Lemma 4.1. Noticing that $C(E) = E$, it may also be deduced from Lemma 4.5.

Lemma 4.8. *For any $x \in [2k+1, 4k]_m$, we have*

$$\frac{x}{2} \in E \iff x \in E^c.$$

Lemma 4.9. *Let $x, y \in (E^c)_0$. If $\widetilde{x}$ and $\widetilde{y}$ are of same parity (respectively of different parity), then the element $\frac{x+y}{2}$ (respectively $\frac{x-y}{2}$) belongs to $(E^c)_0$.*

Proof. From the previous lemma we have $\frac{x}{2}, \frac{y}{2} \in E$. Since E is sum-free we have that both the elements $\frac{x+y}{2}$ and $\frac{x-y}{2} \in E^c$. If $\widetilde{x}$ and $\widetilde{y}$ are of same parity then $\frac{x+y}{2}$ belongs to I_0 and hence to $(E^c)_0$. Similarly if $\widetilde{x}$ and $\widetilde{y}$ are of different parity then $\frac{x-y}{2}$ belongs to I_0 and hence to $(E^c)_0$. Hence the lemma follows. □

Lemma 4.10. *When $\mathrm{card}((\widetilde{E^c})_0) \geq 2$, then $(\widetilde{E^c})_0$ is an arithmetic progression and the common difference d between any two consecutive integers in it is an odd integer.*

Proof. Let $(\widetilde{E^c})_0 = \{\widetilde{x_1} < \widetilde{x_2} < \cdots \widetilde{x_t}\}$. Using Lemma 4.9 it follows that for any i, the elements $\widetilde{x_i}$ and $\widetilde{x_{i+1}}$ are of different parity and

$$x_i = \frac{\widetilde{x_{i-1}} + \widetilde{x_{i+1}}}{2} \ \forall\ 2 \leq i \leq t-1,$$

form which the lemma. □

The following lemma is easy to verify.

Lemma 4.11. *Let $x \in I_0$. If $\widetilde{x}$ is even, then $\frac{x}{2} \in I_{-1}$. If $\widetilde{x}$ is odd, then $\frac{x}{2} \in I_1$.*

On combining lemmas 4.8, 4.10 and 4.11, we obtain

Lemma 4.12. *Let $E \subset \mathbb{Z}/m\mathbb{Z}$ be as above. We then have*

(i) $\widetilde{E}_{-1} = \{\frac{\widetilde{x}}{2} : \widetilde{x} \in (\widetilde{E^c})_0$ *and* $\widetilde{x}$ *is even.*$\}$.

(ii) $\widetilde{E}_1 = \{\frac{m+\widetilde{x}}{2} : \widetilde{x} \in (\widetilde{E^c})_0$ *and* $\widetilde{x}$ *is odd.*$\}$.

(iii) *For any $i \in \{-1, 1\}$, we have*

$$\mathrm{Card}((\widetilde{E^c})_0) - 1 \leq \mathrm{Card}(\widetilde{E}_i) \leq \mathrm{Card}\left((\widetilde{E^c})_0\right).$$

Lemmas 4.12 and 4.10 then give the following result.

Lemma 4.13. *Let $i \in \{-1, 1\}$ and $\mathrm{card}(\widetilde{E}_i) \geq 2$. Then $\mathrm{card}\left((\widetilde{E^c})_0\right) \geq 2$ and $\widetilde{E}_i$ is an arithmetic progression. Moreover, the common difference of the arithmetic progression $\widetilde{E}_i$ is the same as the common difference of the arithmetic progression $(\widetilde{E^c})_0$.*

Lemma 4.14. *If the integer $2k$ does not belong to $\widetilde{E}_{-1}$, then $\widetilde{E}_{-1} = \emptyset$. Similarly if the integer $4k+1$ does not belong to $\widetilde{E}_1$, then $\widetilde{E}_1 = \emptyset$.*

Proof. It is sufficient to prove the claim for $\widetilde{E}_{-1}$, since then for $\widetilde{E}_1$, the claim follows replacing E by $-E$. The assertion follows trivially in case $k = 1$. So we may assume that $k \geq 2$.

Suppose the integer $2k$ does not belong to $\widetilde{E}_{-1}$. Using Lemma 4.12, it follows that $4k \in \widetilde{E}_0$. Since E is sum-free and $2k - 1 \equiv 4k + 4k \pmod{m}$, it follows that $2k - 1$ does not belong to $\widetilde{E}_{-1}$. In case $k = 2$, we have $I_{-1} = \{2k - 1, 2k\}_m$ and hence lemma follows in this case. Therefore we are left to prove the lemma in the case when $k \geq 3$.

We claim that the set $\widetilde{E}_{-1}$ does not contain any odd integer. Suppose the claim is not true and $2k-2r-1$ is the largest odd integer belonging to $\widetilde{E}_{-1}$. Since we know that $2k-1$ can not belong to $\widetilde{E}$, we have $r \geq 1$. Moreover we have $\{2k-2i-1 : 0 \leq i \leq r-1\} \cup \{2k\} \subset \widetilde{E^c}_{-1}$ and hence using Lemma 4.12, $\{4k-2(2i+1) : 0 \leq i \leq r-1\} \cup \{4k\} \subset \widetilde{E}_0$. Hence it follows that $\{8k-2i : 0 \leq i \leq 2r-1\} \subset \widetilde{E}_0 + \widetilde{E}_0$. Since $8k-2i \equiv 2k-2i-1 \pmod{m}$, it follows that $\{2k-2i-1 : 0 \leq i \leq 2r-1\} \subset \widetilde{E^c}$. Since $r \geq 1$, this implies that $2k-2r-1$ can not belong to $\widetilde{E}$. Therefore it follows that $\widetilde{E}_{-1}$ does not contain any odd integer.

Using Lemma 4.13, it follows that $\mathrm{card}(\widetilde{E}_{-1}) \leq 1$. Thus either $\widetilde{E}_{-1} = \emptyset$ or $\widetilde{E}_{-1} = \{2k - 2t\}$. To prove the lemma, we need to rule out the second possibility.

Suppose $\widetilde{E}_{-1} = \{2k-2t\}$ with $t \geq 1$. It follows using Lemma 4.12 that only even integer in $(\widetilde{E^c})_0$ is $4k-4t$. But since E is sum-free we also have $4k-(2k-2t) = 2k+2t$ belong to $(\widetilde{E^c})_0$. Therefore $2k + 2t = 4k - 4t$ and hence $t = \frac{k}{3}$.

The rest of proof is divided into two cases according to whether $t = 1$ or $t \geq 2$. In case $t = 1$ and hence $k = 3$, we have $\widetilde{E}_{-1} = \{4\}$ and the only even integer in $(\widetilde{E^c})_0$ follows that $\widetilde{E}_{-1}$ is an empty set in this case as well. Hence the lemma follows. □

Lemma 4.15. *Let $E \subset \mathbb{Z}/m\mathbb{Z}$ be as above. In case* $\mathrm{card}\left((\widetilde{E^c})_0\right) \geq 3$*, then $E = I_{-1} \cup I_1 = [k+1, 2k]_m \cup [4k+1, 5k]_m$; that is, $2.E = [2k+1, 4k]_m$.*

Proof. The lemma is equivalent to showing that $(\widetilde{E^c})_0 = [2k+1, 4k]$. We prove this by showing that (i) $\{2k+1, 4k\} \subset (\widetilde{E^c})_0$ and (ii) the common difference d between any two consecutive integer in $(\widetilde{E^c})_0$ is equal to 1.

From Lemma 4.12, it follows that $\widetilde{E}_{-1} \neq \emptyset$ as well as $\widetilde{E}_1 \neq \emptyset$. From Lemma 4.14, we have that $\{2k, 4k+1\} \subset \widetilde{E}$. This also implies that $\{2k+1, 4k\} \subset (\widetilde{E^c})_0$.

Moreover, from Lemmas 4.10 and 4.13, the sets $\widetilde{E}_{-1}$ and $(\widetilde{E^c})_0$ are arithmetic progressions with the same common difference d which is an odd integer. In case $d \neq 1$, then $d \geq 3$ and $\{2k+2, 2k+3\} \subset \widetilde{E}$. Since $d \geq 3$, we have $\mathrm{card}(I_{-1}) = k \geq 3$. Let $2k - t$ be the second largest integer belonging to $\widetilde{E}_{-1}$. Then $t \geq 3$ and $\{(2k+2) + 2k - t, (2k+3) + 2k - t\} \subset (\widetilde{E^c})_0$. This implies that $d = 1$, which is contrary to the assumption that $d \neq 1$. Hence the lemma follows.

□

When $G = \mathbb{Z}/m\mathbb{Z}$ and (H, f) is a splitting of G by $\mathbb{Z}/m\mathbb{Z}$, then evidently $H = \{0\}$. Therefore when G is cyclic Theorem 1.2 states the following.

Theorem 4.16. *Let $G = \mathbb{Z}/m\mathbb{Z}$ be a type III group. Let $E \subset \mathbb{Z}/m\mathbb{Z}$ be a sum-free set with* $\mathrm{card}(E) = 2k$*, where $k = \frac{m-1}{6}$. Then for some $d \in (\mathbb{Z}/m\mathbb{Z})^*$ we have that $d.E$ is one of the following three sets.*

(i) $[2k+1, 4k]_m$.

(ii) $\{2k, 4k+1\}_m \cup [2k+2, 4k-1]_m$.

(iii) $[2k, 4k-1]_m$.

Proof. From Proposition 2.2 and Lemma 4.2 we know that there exists $d \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $d.E \subset [k+1, 5k]_m$. Replacing E by $d.E$ we assume that $d = 1$. The proof is divided into four cases according to the cardinality of $(\widetilde{E^c})_0$. In case $\text{card}\left((\widetilde{E^c})_0\right) \geq 3$, then from Lemma 4.15, the set $2.E$ is equal to the set as in (i) of the proposition. In case $\text{card}\left((\widetilde{E^c})_0\right) = 2$, then using Lemma 4.10 and Lemma 4.12 we have that $\text{card}(\widetilde{E}_{-1}) = \text{card}(\widetilde{E}_1) = 1$. Then using Lemma 4.14 we obtain that $\widetilde{E}_{-1} = \{2k\}$ and $\widetilde{E}_1 = \{4k+1\}$. Thus it follows that E is as in (ii) of the proposition. In case $\text{card}\left((\widetilde{E^c})_0\right) = 1$, then replacing E by $-E$, if necessary, and using Lemma 4.12 we have $\text{card}(\widetilde{E}_{-1}) = 1$ and $\text{card}(\widetilde{E}_1) = 0$. Then using Lemma 4.14 we have $\widetilde{E}_{-1} = \{2k\}$ and $\widetilde{E}_1 = \emptyset$. Thus it follows that E is as in (iii) of the proposition. In case $\text{card}\left((\widetilde{E^c})_0\right) = 0$ we have trivially that E is as in (i) of the proposition. □

Now using Theorem 4.16 and Proposition 4.6, we prove Proposition 2.1.

Proof of Proposition 2.1. Let A be a set as in the proposition and $C(A)$ be the subset of $\mathbb{Z}/m\mathbb{Z}$ as above. From Propositions 4.6 and 4.16, we have that there exists $d \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $d.C(A)$ is one of the three sets as given in Proposition 4.16. We then verify that for any $i \notin d^{-1}.[2k, 4k+1]_m$, there always exists $i_1, i_2 \in C(A)$ such that $i = i_1 \pm i_2$. Thus using Proposition 4.6, we have $\alpha_i = 0$ for any $i \notin d^{-1}[2k, 4k+1]_m$. In other words

$$A \subset (df)^{-1}[2k, 4k+1]_m. \tag{16}$$

Therefore (7) holds with $f' = df$. Let $x \in f'^{-1}\{1\}$ and $f" : \mathbb{Z}/m\mathbb{Z} \to G$ be the injective homomorphism satisfying $f''(1) = x$. Then with $H = \ker(f')$ we have that (H, f'') is a splitting of G by $\mathbb{Z}/m\mathbb{Z}$ and

$$A \subset (H, [2k, 4k+1]_m). \tag{17}$$

□

5 Proofs of Theorems 1.2 and 1.4

In this section we prove the following result from which Theorems 1.2 and 1.4 are easily deduced.

Proposition 5.1. *Let A be as in Theorem 1.4. Then there exists a splitting (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$ and a subgroup K of H, such that the following holds. With L being one of the following sets, $L(H, f, 0), L(H, f, K, I), L(H, f, K, II)$, (see Definition 1.3) we have* $\text{card}(A \setminus L) \leq 4\epsilon n$.

Let A be as in Proposition 5.1. From Proposition 2.1 there exists a splitting (H, f') of G by $\mathbb{Z}/m\mathbb{Z}$ such that

$$A \subset (H, [2k, 4k+1]_m).$$

It is easy to verify that $A \cup (H, [2k+1, 4k-1]_m)$ is a sum-free subset of G. Without any loss of generality we may assume that A is a maximal (with respect to set inclusion)

sum-free set. Therefore A is equal to the union of $(H, [2k+1, 4k-1]_m)$ and the following set:

$$(A_{2k}, \{2k\}_m) \cup (A_{2k+1}, \{2k+1\}_m) \cup (A_{4k}, \{4k\}_m) \cup (A_{4k+1}, \{4k+1\}_m), \tag{18}$$

with $A_{2k}, A_{2k+1}, A_{4k}, A_{4k+1}$ being subsets of H. For any $i \in \{2k, 4k+1\}_m$, applying Lemma 4.4 with $i_0 = 2i$, we obtain the following inequality:

$$\mathrm{Card}(A_i) + \mathrm{Card}(A_{2i}) \geq \frac{n}{m} - \epsilon n. \tag{19}$$

Lemma 5.2. *If for some $i \in \{2k, 4k+1\}_m$, we have $\mathrm{card}(A_i) > 2\epsilon n$, then $\mathrm{card}(A_i + A_i) < \frac{3}{2}\,\mathrm{card}(A_i)$.*

Proof. Since A is sum-free, the set $A_{2i} \subset H \setminus (A_i + A_i)$. Using this and (19), the lemma follows after a small calculation. □

Using Lemmas 5.2 and 3.2, we obtain the following result.

Corollary 5.3. *If for some $i \in \{2k, 4k+1\}_m$, we have $\mathrm{card}(A_i) > 2\epsilon n$, then A_i is contained in a coset of the stabiliser K_i in H of the subset $A_i + A_i$ of H; in other words, there exists an element $x_i \in H$ such that $A_i \subset K_i + x_i$ and $A_i + A_i = K_i + 2x_i$.*

Lemma 5.4. *If $\min(\mathrm{Card}(A_{2k}), \mathrm{Card}(A_{4k+1})) > 2\epsilon n$, then*

$$A_{4k+1} + A_{4k+1} = -(A_{2k} + A_{2k}).$$

Indeed there exists a subgroup K of H and an element $x \in H$ such that $A_{2k} \subset K + x$, $A_{4k+1} \subset K - x$, $A_{2k} + A_{2k} = K + 2x$ and $A_{4k+1} + A_{4k+1} = K - 2x$.

Proof. Let K_{2k}, K_{4k+1} be the subgroups and x_{2k}, x_{4k+1} be the elements in H as given by Corollary 5.3. To prove the lemma, we shall show that $K_{2k} = K_{4k+1}$ and $x_{2k} + x_{4k+1} \in K_{2k}$. The lemma follows from this with the choice of $K = K_{2k}$ and $x = x_{2k}$.

First we prove the following facts:

$$A_{2k} - A_{4k} = H \setminus (K_{2k} - x_{2k}) \tag{20}$$

$$A_{4k+1} - A_{2k+1} = H \setminus (K_{4k+1} - x_{4k+1}). \tag{21}$$

Using the fact that $A_{4k} \subset H \setminus (K_{2k} + 2x_{2k})$ and $A_{2k} \subset K_{2k} + x_{2k}$, it follows that

$$A_{2k} - A_{4k} \subset H \setminus (K_{2k} - x_{2k}). \tag{22}$$

Since $A_{2k} \subset K_{2k} + x_{2k}$, we obtain that $\mathrm{card}(K_{2k}) > 2\epsilon n$. Therefore it follows that $\mathrm{card}(A_{2k}) > \frac{\mathrm{card}(K_{2k})}{2}$. Let $y \in H$ be such that $K_{2k} + y \neq K_{2k} + 2x_{2k}$. Using (19), it follows that $\mathrm{card}(A_{4k} \cap (K_{2k} + y)) > \frac{\mathrm{card}(K_{2k})}{2}$.

Therefore using Lemma 3.1, it follows $(K_{2k} + x_{2k}) - (K_{2k} + y) \subset A_{2k} - A_{4k}$ for any y as above. Using this and (22), we obtain (20). Using the similar arguments, we obtain (21).

Since A is sum-free, it follows that $A_{2k} - A_{4k}$ and A_{4k+1} are disjoint subsets of H. Hence we obtain from (20) that $A_{4k+1} \subset K_{2k} - x_{2k}$. Therefore

$$K_{4k+1} + 2x_{4k+1} = A_{4k+1} + A_{4k+1} \subset K_{2k} - 2x_{2k}.$$

It follows that $K_{4k+1} \subset K_{2k}$ and $x_{2k} + x_{4k+1} \in K_{2k}$. Similar arguments imply that $K_{4k+1} \subset K_{2k}$. Hence the lemma follows.

□

The following lemma is easy to verify.

Lemma 5.5. *Let (H, f') be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$ and $x \in H$. Further let $f : \mathbb{Z}/m\mathbb{Z} \to G$ be the injective homomorphism with $f(2k) = f'(2k) + x$. Then H is a supplement of image of f in G. Moreover given any $B \subset H$ and $\lambda \in \mathbb{Z}$ we have*

$$(B + \lambda x, \{\lambda 2k\}_m)_{(H,f')} = (B, \{\lambda 2k\}_m)_{(H,f)}.$$

Proof of Proposition 5.1. From Proposition 2.1, there exists a splitting (H, f') of G by $\mathbb{Z}/m\mathbb{Z}$ such that A is equal to the set as in (18). The proof of the proposition is divided into the following four cases.

When $\mathrm{card}(A_{2k}) \leq 2\epsilon n$ and $\mathrm{card}(A_{4k+1}) \leq 2\epsilon n$: In this case with $L = L(H, f')$, we have

$$\mathrm{card}(A \setminus L) = \mathrm{card}(A_{2k}) + \mathrm{card}(A_{4k+1}) \leq 4\epsilon n.$$

Hence the proposition follows in this case.

When $\mathrm{card}(A_{2k}) > 2\epsilon n$ and $\mathrm{card}(A_{4k+1}) \leq 2\epsilon n$: Let K_{2k} be a subgroup and $x_{2k} \in H$ be as in Lemma 5.3. Let $f : \mathbb{Z}/m\mathbb{Z} \to G$ be the injective homomorphism with $f(2k) = f'(2k) + x_{2k}$. With $L = L(H, f, K, I)$, where $K = K_{2k}$, using Lemma 5.5, it follows that

$$\mathrm{card}(A \setminus L) = \mathrm{card}(A_{4k+1}) \leq 2\epsilon n.$$

Hence the proposition follows in this case.

When $\mathrm{card}(A_{2k}) \leq 2\epsilon n$ and $\mathrm{card}(A_{4k+1}) > 2\epsilon n$: Replacing (H, f') by $(H, -f')$, the proposition follows using the arguments of the previous case.

When $\mathrm{card}(A_{2k}) > 2\epsilon n$ and $\mathrm{card}(A_{4k+1}) > 2\epsilon n$: Let K be a subgroup and $x \in H$ be as in Lemma 5.4. Let $f : \mathbb{Z}/m\mathbb{Z} \to G$ be the injective homomorphism with $f(2k) = f'(2k) + x$. Then using Lemmas 5.4 and 5.5, it follows that $A \subset L(H, f, K, II)$. Hence the proposition follows in this case.

□

6 Proof of Theorem 1.5

Recall that $\mathcal{L}(G)$ denotes the family of sum-free subsets of the largest cardinality in G. We choose a splitting (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$ and write $\mathcal{R}(H)$ to denote the collection of subgroups of H. We use $L, L_1, L_2, ...$ to denote elements in $\mathcal{L}(G)$ and use $K_1, K_2, ...$ to denote elements in $\mathcal{R}(H)$.

Given $h \in \mathrm{Aut}(G)$ and for any $L \in \mathcal{L}(G)$, we have that $h(L)$ also belong to $\mathcal{L}(G)$. This defines an action of $\mathrm{Aut}(G)$ on $\mathcal{L}(G)$. Given $L_1, L_2 \in \mathcal{L}(G)$, we say that $L_1 \sim L_2$ if L_1 and L_2 are in the same orbit.

Given $h \in \mathrm{Aut}(H)$ and for any $K \in \mathcal{R}(H)$, we have that $h(K) \in \mathcal{R}(H)$. This defines an action of $\mathrm{Aut}(H)$ on $\mathcal{R}(H)$. We say $K_1 \sim K_2$, where $K_1, K_2 \in \mathcal{R}(H)$, if K_1 and K_2 are in the same orbit. In this section, we shall prove Theorem 1.5 which relates the number of orbits in $\mathcal{L}(G)$ to the number of orbits in $\mathcal{R}(H)$.

We have the following two maps

$$T_1, T_2 : \mathcal{R}(H) \to \mathcal{L}(G) \tag{23}$$

with $T_1(K) = L(H, f, K, I)$ and $T_2(K) = L(H, f, K, II)$ for any $K \in \mathcal{R}(H)$. We say that $L \in \mathcal{L}(G)$ has a *presentation* with respect to (H, f) if

$$L \in \mathrm{Im}(T_1) \cup \mathrm{Im}(T_2) \cup \{L(H, f, 0)\}.$$

Lemma 6.1. *Given $L \in \mathcal{L}(G)$, there exists $L_1 \in \mathrm{Im}(T_1) \cup \mathrm{Im}(T_2) \cup \{L(H, f, 0)\}$ such that $L \sim L_1$.*

Proof. From Theorem 1.2, there exists a splitting (H', f') of G by $\mathbb{Z}/m\mathbb{Z}$ such that L is one of the following sets $L(H', f', 0), L(H', f', K', I), L(H', f', K', II)$ with K' being a subgroup of H'. It is easy to verify that there exists $h \in \mathrm{Aut}(G)$ such that $h(H') = H$, $h(\mathrm{Im}(f')) = \mathrm{Im}(f)$ and $h(f'(1)) = f(1)$. Then $h(L)$ is equal to one of the following sets: $L(H, f, 0)$, $T_1(h(K'))$, $T_2(h(K'))$. Hence the lemma follows. □

In this section we shall prove the following results.

Proposition 6.2. *Let G be a finite abelian group of type III and the exponent m of G is not 7. Let $i \in \{1, 2\}$ and $K_1, K_2 \in \mathcal{R}(H)$. Then the following holds:*

$$T_i(K_1) \sim T_i(K_2) \iff K_1 \sim K_2, \tag{24}$$

$$T_1(K_1) \nsim T_2(K_2), \tag{25}$$

$$L(H, f, 0) \nsim T_i(K_1). \tag{26}$$

Proposition 6.3. *Let G be a finite abelian group of type III and the exponent m of G is 7; in other words, let $G = (\mathbb{Z}/7\mathbb{Z})^r$. Let $i \in \{1, 2\}$ and $K_1, K_2 \in \mathcal{R}(H)$. Then the following holds:*

$$T_i(K_1) \sim T_i(K_2) \iff K_1 \sim K_2, \tag{27}$$

$$T_1(K_1) \nsim T_2(K_2), \tag{28}$$

$$L(H, f, 0) \sim T_i(K_1) \iff K_1 = H \,and\, i = 2. \tag{29}$$

Using Lemma 6.1, Propositions 6.2 and 6.3, it may be verified easily that Theorem 1.5 follows.

Lemma 6.4. *Let $K_1, K_2 \in \mathcal{R}(H)$. Then for any $i \in \{1, 2\}$, we have*

$$K_1 \sim K_2 \implies T_i(K_1) \sim T_i(K_2).$$

Proof. Since $K_1 \sim K_2$, there exists $h \in \mathrm{Aut}(H)$ with $h(K_1) = h(K_2)$. Moreover since $G = H \oplus \mathrm{Im}(f)$, we may extend h to $\tilde{h} \in \mathrm{Aut}(G)$ by defining $\tilde{h}$ to be the identity map on $\mathrm{Im}(f)$. Then it is easy to verify that $\tilde{h}(T_i(K_1)) = T_i(K_2)$. Hence the lemma follows. □

Using Lemmas 6.1 and 6.4 we obtain that

$$\mathrm{Card}(\mathcal{L}(G)/\mathrm{Aut}(G)) \leq 2\mathrm{Card}(\mathcal{R}(H)/\mathrm{Aut}(H)) + 1. \tag{30}$$

Recall that for any subset A of a finite abelian group G the *stabiliser* $S(A)$ of A in G is the subset of G consisting of those elements $g \in G$ such that $g + A = A$. Given any element $x \in G$, there exists a unique element $x_1 \in H$ and $x_2 \in \mathbb{Z}/m\mathbb{Z}$ such that $x = x_1 + f(x_2) := (x_1, x_2)$. Let $\pi_2 : G \to \mathbb{Z}/m\mathbb{Z}$ be the map given by $\pi_2(x) = \pi_2((x_1, x_2)) = x_2$.

Lemma 6.5. *Let L be a set in $\mathcal{L}(G)$ which has a presentation with respect to (H, f). Then for any subset A of L, the stabiliser $S(A)$ of A in G is contained in H.*

Proof. The lemma is equivalent to showing that $\pi_2(S(A)) = \{0\}$, which is equivalent to showing that $\mathrm{card}(\pi_2(S(A))) = 1$. In case $\mathrm{card}(\pi_2(S(A))) = d$, then $\pi_2(S(A))$ consists of the image in $\mathbb{Z}/m\mathbb{Z}$ of all the integers in divisible by $\frac{m}{d}$. Now clearly we have that the set $\pi_2(A)$ is invariant under the translation by the elements in $\pi_2(S(A))$. Therefore if t is any integer such that its residue modulo m belong to $\pi_2(A)$, then for any integer i, the residue modulo m of the integer $t + i\frac{m}{d}$ belongs to $\pi_2(A)$. Since $A \subset L$, we have $\pi_2(A) \subset [2k, 4k+1]_m$. Let t be the largest integer in $[2k, 4k+1]$ such that its residue modulo m belongs to $\pi_2(A)$. Since $t + \frac{m}{d}$ also belongs to $\pi_2(A)$, it follows that

$$t + \frac{m}{d} \geq 2k + m = 8k + 1.$$

In case $d \neq 1$, then since G is of type III, we have d is at least 7. Then since t is at most $4k+1$, the left hand side of the above inequality is at most $4k + 1 + \frac{6k+1}{7}$, which is strictly less than the right hand side of the the above inequality, which is absurd. Thus $\mathrm{card}(\pi_2(S(A)) = d = 1$. Hence the lemma follows. □

Using Lemma 6.5, the following result is easily obtained.

Corollary 6.6. *The stabiliser of $L(H, f, 0)$ in G is H and the stabiliser of $T_i(K)$ in G is K for any $i \in \{1, 2\}$.*

We say that a subset A of G is *almost translation invariant* if it is invariant under translation by more than $\frac{n}{m}$ elements of G; that is, if $\mathrm{card}(S(A)) \geq \frac{n}{m}$. Using Lemma 6.5, we also obtain the following result.

Corollary 6.7. *Let $L \in \mathcal{L}(G)$ has a presentation with respect to (H, f). The stabiliser of any nonempty almost translation invariant subsets of L is H.*

6.1 Proof of Proposition 6.2

In this subsection we shall assume that the exponent m of G is not 7.

Lemma 6.8. *Given any $L \in \mathcal{L}(G)$, there exists a nonempty almost translation invariant subset of L.*

Proof. Since m is not 7, the set $[2k+2, 4k-1]_m$ is a nonempty set, where $k = \frac{m-1}{6}$. Using this we verify that the set $(H, [2k+2, 4k-1]_m)$ is a non-empty almost translation invariant subset of L. □

Corollary 6.9. *Let $L_1, L_2 \in \mathcal{L}(G)$ have presentation with respect to (H, f). If $h \in \mathrm{Aut}(G)$ with $h(L_1) = L_2$, then $h(H) = H$.*

Proof. From Lemma 6.8, there exist a nonempty almost translation invariant subset B of L_1. From Corollary 6.7, the stabiliser of B in G is H. Since $h(L_1) = L_2$, it follows that $h(B)$ is an almost translation invariant subset of L_2 and the stabiliser of $h(B)$ in G is $h(H)$. Using Corollary 6.7, it follows that $h(H) = H$. Hence the claim follows. □

Let C_0, C_1, C_2 are subsets of $\mathbb{Z}/m\mathbb{Z}$ as follows.

$$C_0 = [2k+1, 4k]_m, \quad C_1 = [2k, 4k-1]_m, \quad C_2 = \{2k\}_m \cup [2k+2, 4k-1]_m \cup \{4k+1\}_m. \quad (31)$$

Lemma 6.10. *When $m \neq 7$, the sets C_0, C_1, C_2 lie in different orbits under the action of $Aut(\mathbb{Z}/m\mathbb{Z})$.*

Proof. It is easy to verify that $C_0 = -C_0$ and $C_2 = -C_2$, whereas $C_1 \neq -C_1$. Therefore C_1 could neither lie in the same orbit as C_0 nor it could lie in the same orbit as C_2. We may verify that the cardinality of $C_0 + C_0$ is equal to $4k - 2$, whereas the cardinality of $C_2 + C_2$ is equal to $4k$. Since $k = \frac{m-1}{6} \neq 1$, we obtain that $\text{card}(C_0 + C_0) \neq \text{card}(C_2 + C_2)$. Hence C_0 could not be in the same orbits as C_2. Thus the lemma follows. □

Lemma 6.11. *For any $i \in \{1, 2\}$, and $K_1, K_2 \in \mathcal{R}(H)$, we have*

$$T_i(K_1) \sim T_i(K_2) \implies K_1 \sim K_2.$$

Proof. Let $h \in \text{Aut}(G)$ with $h(T_i(K_1)) = T_i(K_2)$. To prove the lemma, we need to show that there exists $h' \in \text{Aut}(H)$ with $h'(K_1) = h'(K_2)$. From Corollary 6.9 we have $h(H) = H$. Therefore the restriction h' of h to H is an automorphism of H. From Corollary 6.6, the stabiliser of $T_i(K_1)$ in G is K_1. Therefore it follows that $h(K_1)$ which is same as $h'(K_1)$ is the stabiliser of $T_i(K_2)$. But from Corollary 6.6, the stabiliser of $T_i(K_2)$ in G is K_2. Therefore $h'(K_1) = K_2$. Hence the lemma follows. □

The following lemma is easy to verify.

Lemma 6.12. *Let $h \in \text{Aut}(G)$ with $h(H) = H$. Then the restriction of $\pi_2 h$ to $\text{Im}(f)$ is an automorphism of $\text{Im}(f)$. Moreover for any $A \subset G$, we have $\pi_2 h \pi_2(A) = \pi_2 h(A)$.*

Lemma 6.13. *For any $K_1, K_2 \in \mathcal{R}(H)$, we have*

$$T_1(K_1) \nsim T_2(K_2).$$

Proof. Suppose the lemma is not true and there exist $K_1, K_2 \in \mathcal{R}(H)$ such that $T_1(K_1) \sim T_2(K_2)$. We claim that this implies that $\pi_2 T_1(K_1)$ and $\pi_2 T_2(K_2)$ are in the same orbit under the action of $\text{Aut}(\text{Im}(f))$.

There exist $h \in \text{Aut}(G)$ with $h(T_1(K_1) = T_2(K_2)$. Therefore we have $\pi_2 h(T_1(K_1)) = \pi_2(T_2(K_2))$. From Corollary 6.9, we have $h(H) = H$. Using Lemma 6.12 it follows that $\pi_2 h \pi_2(T_1(K_1)) = \pi_2 h(T_1(K_1)) = \pi_2 T_2(K_2)$. Therefore the restriction of $\pi_2 h$ to $\text{Im}(f)$ is an automorphism of $\text{Im}(f)$ which transports $\pi_2 T_1(K_1)$ to $\pi_2 T_2(K_2)$. Hence the claim follows.

Unless $K_1 = K_2 = H$, $\text{Card}(\pi_2(T_1(K_1))) \neq \pi_2(T_2(K_2))$. Therefore it follows that $K_1 = K_2 = H$. Therefore $\pi_2(T_1(K_1)) = f(C_1)$ and $\pi_2(T_2(K_2)) = f(C_2)$, where $C_1, C_2 \subset \mathbb{Z}/m\mathbb{Z}$ as defined above. The lemma follows using Lemma 6.10. □

Using the arguments similar to those used in the proof of Lemma 6.13, we obtain the following lemma.

Lemma 6.14. *For any $K \in \mathcal{R}(H)$ and $i \in \{1, 2\}$, we have*

$$L(H, f, 0) \nsim T_i(K).$$

Using Lemmas 6.4, 6.11, 6.13 and 6.14, we obtain Proposition 6.2.

6.2 Proof of Proposition 6.3

In this subsection, we shall assume that the exponent m of G is 7; that is $G = (\mathbb{Z}/7\mathbb{Z})^r$.

Lemma 6.15. *Let $L \in \mathcal{L}(G)$ has a presentation with respect to (H, f). When $L \neq T_2(K)$ with K being a proper subgroup of H, then also there exists a nonempty almost translation invariant subset of L. When $L = T_2(K)$ with K being a proper subgroup of H, there does not exists any nonempty almost translation invariant subset of L.*

Proof. When $L \in \mathrm{Im}(T_1) \cup \{L(H, f, 0)\}$, then $(H, \{3\}_7)$ is a nonempty almost translation invariant subset of L. When $L = T_2(H)$, then L is a nonempty almost translation invariant subset of L. This proves the first claim. Using Lemma 6.5, the second claim follows easily. □

Lemma 6.16. *When $L = T_2(K)$ for some $K \in \mathcal{H}$ with $K \neq H$, then the there exists a nonempty almost translation invariant subset of $L + L$. Further the stabiliser of any nonempty almost translation invariant subset of $L + L$ in G is H.*

Proof. Since K is a proper subgroup, we have that $\mathrm{card}(K) \leq \frac{\mathrm{card}(H)}{7}$ and hence $\mathrm{card}(K^c) \geq \frac{6\,\mathrm{card}(H)}{7} > \frac{\mathrm{card}(H)}{2}$. Therefore $K^c + K^c = H$. Using this we verify that

$$L + L = (H, [-1, 1]_7) \cup (K^c, 2) \cup (K, 3) \cup (K, 4), (K^c, 5).$$

Therefore $(H, [-1, 1]_7)$ is an almost translation invariant subset of $L + L$. This proves the first claim.

We shall prove the lemma by showing that for any nonempty subset A of $L + L$, we have that $\pi_2(S(A)) = \{0\}$. If not then for some subset A of $L + L$ we have $\pi_2(S(A)) = \mathbb{Z}/7\mathbb{Z}$. This implies that there are elements $x, y \in H$ such that $(x, 1) \in S(A)$ and $(y, 0) \in A$.

Then it follows that all the elements $(y + 4x, 4), (y + 5x), (y + 3x) \in L$. This implies that the elements $y + 4x$ and $y + 3x$ belongs to K whereas the element $y + 5x$ belongs to K^c. Thus the element $y + 5x - (y + 4x) = x$ belongs to $K^c - K = K^c$. On the other hand $y + 4x - (y + 3x)$ belongs to $K - K = K$. Thus the element x belongs to the set K as well as its complement, which is not possible. Hence $\pi_2(S(A)) = \{0\}$. Hence the lemma follows. □

Remark 6.17. From Lemmas 6.15, 6.16 and Corollary 6.7, the following result follows. If $L \in \mathcal{L}(G)$ has a presentation with respect to splittings (H_1, f_1) and (H_2, f_2) of G by $\mathbb{Z}/m\mathbb{Z}$, then $H_1 = H_2$.

Let $C_0 = [3, 4]_7$, $C_1 = [2, 3]_7$ and $C_2 = \{2, 4\}_7$.

Lemma 6.18. *The set $C_0 = 2C_2$ and $L(H, f, 0) = 2T_2(H)$. The set C_1 and C_0 lie in different orbits under the action of* $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$.

Using Lemmas 6.15, 6.16, 6.18 and arguments similar to those used in the proof of Proposition 6.2, we obtain Proposition 6.3.

7 Proof of Theorem 1.6

If $m = \prod_{p|m} p^{v_p(m)}$ then $H = \bigoplus_{p|m} H_p$ with $H_p = (\mathbb{Z}/p^{v_p(m)}\mathbb{Z})^r$ and we have

$$\mathrm{Card}(\mathcal{H}/Aut(H)) = \prod_p \mathrm{Card}(\mathcal{H}_p/Aut(H_p)), \tag{32}$$

where $\mathcal{H}_p$ denotes the family of subgroups of H_p. Therefore we may assume that H is a p-group.

A finite commutative p-group is called homogeneous of height t and rank r if it is isomorphic to the direct sum of r copies of the cyclic group $\mathbf{Z}/p^t\mathbf{Z}$, where $t \geq 0$ and $r \geq 1$ are integers. Thus H_p is a homogeneous group of height $v_p(m)$ and rank r.

We will show that $\mathrm{Aut}(H_p)$ acts transitively on isomorphism classes of subgroups of H_p. Thus if K_1 and K_2 are isomorphic subgroups of H_p then there exists an automorphism of H_p that transports K_1 onto K_2.

We shall consider H_p endowed with its natural $\mathbf{Z}$-module structure. Let F be the free $\mathbf{Z}$-module of rank r and M be the submodule $p^{v_p(m)}F$ of F. Then M is free $\mathbf{Z}$-module of rank r and H_p is isomorphic to F/M. Let f be an isomorphism from F/M onto H_p and let ϕ denote $f.p$, where p is the canonical projection from F onto F/M. Thus ϕ is a surjective homomorphism of $\mathbf{Z}$-modules from F onto H_p with $\mathrm{Ker}(\phi) = M$.

Proposition 7.1. *When E is a submodule of F containing M there exists a $\mathbf{Z}$-basis $\{e_1, e_2, \ldots, e_r\}$ for F and an increasing sequence of integers $0 \leq a_1 \leq a_2 \leq \ldots \leq a_r \leq v_p(m)$ such that*

(i) *$\{p^{a_1}e_1, p^{a_2}e_2, \ldots, p^{a_r}e_r\}$ is a $\mathbf{Z}$-basis for E.*

(ii) *E/M is isomorphic to $\bigoplus_{1\leq i\leq r} \mathbf{Z}/p^{t-a_i}\mathbf{Z}$.*

Proof. Since E contains M, E is a submodule of F of rank r. From the theory of modules over principal ideal domains it follows that there is a $\mathbf{Z}$-basis $\{e_1, e_2, \ldots, e_r\}$ of F and an increasing sequence of integers $0 \leq n_1 \leq n_2 \ldots \leq n_r$ such that $\{n_1e_1, n_2e_2, \ldots, n_re_r\}$ is a $\mathbf{Z}$-basis for E.

Since $p^{v_p(m)}e_1 + p^{v_p(m)}e_2 + \ldots + p^{v_p(m)}e_r$ is in M and therefore in E, there exist integers c_i, $1 \leq i \leq r$, such that

$$p^{v_p(m)}e_1 + p^{v_p(m)}e_2 + \ldots + p^{v_p(m)}e_r = c_1n_1\, e_1 + c_2n_2\, e_2 + \ldots + c_rn_r\, e_r\,. \tag{33}$$

Equating the coefficients of the e_i we deduce that, for each i, $1 \leq i \leq r$, that n_i divides $p^{v_p(m)}$. On setting $n_i = p^{a_i}$ for each i, $1 \leq i \leq r$, we see that $\{a_i\}_{1\leq i\leq r}$ is an increasing sequence of integers in the interval $[0, t]$ satisfying (i). Also (ii) is verified by noting that M is generated by $\{p^{v_p(m)}e_1, p^{v_p(m)}e_2, \ldots, p^{v_p(m)}e_r\}$ and passing to quotients. □

Proposition 7.2. *If K_1 and K_2 are isomorphic subgroups of a homogeneous H_p then there exists an automorphism of H_p that transports K_1 onto K_2.*

Proof. K_1 and K_2 are $\mathbf{Z}$-submodules of H_p viewed as a $\mathbf{Z}$-module. Let E_1 and E_2 be the inverse images of K_1 and K_2 under ϕ. Then E_1 and E_2 are submodules of F containing M. Proposition 1 shows that there are bases $\{e_1, e_2, \ldots, e_r\}$ and $\{f_1, f_2, \ldots, f_r\}$ of F, increasing sequences $\{a_i\}_{1\leq i\leq r}$ and $\{b_i\}_{1\leq i\leq r}$ of integers in the interval $[0, k]$ such that $\{p^{a_1}e_1, p^{a_2}e_2, \ldots, p^{a_r}e_r\}$ is a $\mathbf{Z}$-basis for E_1 and $\{p^{b_1}f_1, p^{b_2}f_2, \ldots, p^{b_r}f_r\}$ is a $\mathbf{Z}$-basis for E_2. Moreover

$$\bigoplus_{1\leq i\leq r} \mathbf{Z}/p^{k-a_i}\mathbf{Z} \;\cong\; E_1/M \;\cong\; K_1 \;\cong K_2 \;\cong\; E_2/M \;\cong\; \bigoplus_{1\leq i\leq r} \mathbf{Z}/p^{k-b_i}\mathbf{Z}\,, \tag{34}$$

from which we have that $a_i = b_i$, for each i, $1 \leq i \leq r$. Thus if θ is the automorphism of F defined by $\theta(e_i) = f_i$, for each $1 \leq i \leq r$, then θ transports E_1 onto E_2 and leaves M stable. On passing to quotients θ thus defines an automorphism of H_p that transports K_1 onto K_2. □

One may easily verify the following lemma.

Lemma 7.3. *The number of isomorphism classes of subgroups of H_p is equal to $\binom{v_p(m)+r}{r}$.*

Combining (32), Proposition 7.2 and Lemma 7.3 we obtain.

Proposition 7.4. *When $H = (\mathbb{Z}/m\mathbb{Z})^r$ then we have*

$$\mathrm{Card}(\mathcal{H}/Aut(H)) = \prod_{p^{v_p(m)}||m} \binom{v_p(m)+r}{r}.$$

Combining Proposition 7.4 and Theorem 1.5, Theorem 1.6 follows.

8 Proof of Theorem 1.8.

The main result we are required to prove Theorem 1.8 is the following result. The arguments used in proving it are similar to those used by Green and Ruzsa in proving [5, Lemma 5.8].

Proposition 8.1. *Let G be a finite abelian group of type III and exponent m. With $o_m(2^{c(G)})$ exceptions, all sum-free $A \subset G$ are described as follows. Choose a splitting (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$ and take A to be a subset of $(H, [2k, 4k+1]_m)$, where $k = \frac{m-1}{6}$.*

Presently, we state and prove a few results required to deduce Theorem 1.8 from Proposition 8.1. The following lemma is easy to verify.

Lemma 8.2. *The number of splittings (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$ is at most $nm \log n$.*

Lemma 8.3. *Let (H, f) be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$. The number of sum-free subsets A of G with $A \subset (H, [2k, 4k+1]_m)$ is at most $a(H)2^{c(G)}$.*

Proof. If $A \subset (H, [2k, 4k+1]_m)$, then $A = \bigcup_{i \in [2k, 4k+1]_m} (A_i, i)$ with $A_i's$ being subset of H. Since A is sum-free, $A_{4k} \subset H \setminus (A_{2k} + A_{2k})$ and $A_{2k+1} \subset H \setminus (A_{4k+1} + A_{4k+1})$. Therefore given any $B_1 \in S(k_1, k_2, H)$ and $B_2 \in S(k_1'k_2', H)$, the number of $A's$, with $A_{2k} = B_1$ and $A_{4k+1} = B_2$, is at most $\frac{1}{2^{k_2+k_2'}} 2^{c(G)}$. Using this and the definition of $a(H)$, the lemma follows. □

Lemma 8.4. *Let (H, f) be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$. The number of sum-free subsets A of G with $A \subset (H, [2k, 4k]_m)$ is equal to $a(H)2^{c(G)}$.*

Proof. It is easy to verify that any $A = \bigcup_{i \in [2k, 4k]_m} (A_i, i)$ with $A_{4k} \subset H \setminus (A_{2k} + A_{2k})$ is a sum-free subset of G. For any $B \in S(k_1, k_2, H)$, the number of such $A's$ with $A_{2k} = B$ is equal to $\frac{1}{2^{k_2}} 2^{c(G)}$. Moreover for different choices of B, the sets A are different. Hence the lemma follows. □

Combining Proposition 8.1 and Lemmas 8.2, 8.3, 8.4, we obtain Theorem 1.8.

Lemma 8.5. *With $o_m(2^{\mu(G)n})$ exceptions, the rest of sum-free $A \subset G$ are described as follows. For some sum-free subset L of the largest cardinality in G, the set A is almost contained in L; that is $A = B \cup C$ with $B \subset L$ and $C \subset G$ with $\mathrm{card}(C) = o_m(n)$.*

Proof. Let $\mathcal{F}$ be a family of subsets of G as provided by Lemma 3.4. Then it is clear that except $o(2^{\mu(G)n})$ sets, the rest of sum-free subsets A are subsets of some $F_i \in \mathcal{F}$ with $\mathrm{card}(F_i) \geq \mu(G)n - \frac{n}{(\ln n)^{1/17}}$. Using this, Lemma 3.3 and Theorem 1.4, the lemma follows. □

Lemma 8.6. *When G is a finite abelian group of type III which is of cardinality n and exponent m, the total number of sum-free subsets of the largest cardinality in G is at most $3nm \log n 2^{\log^2 n}$.*

Proof. From Theorem 1.2, any $L \in \mathcal{L}(G)$ has a presentation with respect to some splitting (H, f) of G by $\mathbb{Z}/m\mathbb{Z}$. The number of L which has a presentation with respect to a splitting (H, f) is no more than thrice the number of subgroups of H. The number of subgroups of H is at most $2^{\log^2 n}$. Therefore using Lemma 8.2, the lemma follows.

□

Given any subset L of G and an elements $x \in G$, let $R(x, L)$ be a collection of pairwise disjoint two element subsets B of L such that x is either sum or difference of elements in B. Moreover we assume that among all possible such collection, $R(x, L)$ is of largest possible cardinality. The following lemma is easy to verify.

Lemma 8.7. *For any $i \in \mathbb{Z}/m\mathbb{Z}$ with $i \notin [2k, 4k+1]_m$, there exists $i_1, i_2 \in [2k+1, 4k]_m$, with $i_1 \neq i_2$ such that either $i = i_1 + i_2$ or $i = i_1 - i_2$.*

8.1 When m is not 7.

In this section we shall prove Proposition 8.1 in the case when the exponent m of G is not 7. The following lemma is easy to verify.

Lemma 8.8. *For any $i \in \mathbb{Z}/m\mathbb{Z}$ with $i \notin [2k, 4k+1]_m$, there exists $i_1, i_2 \in [2k, 4k-1]_m$, with $i_1 \neq i_2$ such that either $i = i_1 + i_2$ or $i = i_1 - i_2$.*

Lemma 8.9. *Let the exponent m of G is not 7 and $L \in \mathcal{L}(G)$. Let (H, f) be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$ such that L has a presentation with respect to (H, f). Then for any element $x \in G$ with $x \notin (H, [2k, 4k+1]_m)$, the cardinality of $R(x, L)$ is at least $\frac{5n}{7m}$.*

Proof. If $x \notin (H, [2k, 4k+1]_m)$, then $x = (x_1, x_2)$ with $x_2 \notin [2k, 4k+1]_m$. We verify that there exists a proper subgroup K of G such that the following holds. Either $(H \setminus K, [2k+1, 4k]_m) \subset L$ or $(H, [2k, 4k-1]_m) \subset L$. Using Lemmas 8.7 and 8.8, it follows that

$$\mathrm{card}(R(x, L)) \geq \mathrm{card}(H) - 2\,\mathrm{card}(K) \geq \frac{5n}{7m}.$$

The last inequality follows using the fact that since K is a proper subgroup of the type III group H, we have $\mathrm{card}(K) \leq \frac{\mathrm{card}(H)}{7}$. Hence the lemma follows. □

Lemma 8.10. *Let $L \in \mathcal{L}(G)$. Let (H, f) be a splitting of G by $\mathbb{Z}/m\mathbb{Z}$ as given by Lemma 8.9. The number of sum-free $A \subset G$*

$$\textit{with } \mathrm{card}(A \setminus L) = o_m(n) \textit{and } A \not\subset \ (H, [2k, 4k+1]_m)$$

is $O(2^{c(G) - c(m)n})$, where $c(m) > 0$ is a constant depending only upon m.

Proof. Given any $x \notin (H, [2k, 4k+1]_m)$, first we obtain an upper bound for the number of $A's$ containing x. Since A is sum-free, it may contain at most one element from the pair of elements $(y_1, y_2) \in R(x, L)$. Therefore we obtain that when A contains x, the number of possibilities for $A \cap L$ is $2^{c(G)-2\,\mathrm{card}(R(x,L))}3^{\mathrm{card}(R(x,L))}$. Since $\mathrm{card}(A \setminus L) = o_m(n)$, the number of possibile subsets A containing x is at most

$$2^{o_m(n)}2^{c(G)-(2-\log 3)\,\mathrm{Card}(R(x,L))}.$$

Since the total number of choices for x is at most n, using Lemma 8.9 we obtain the lemma. □

Combining Lemmas 8.5, 8.6 and 8.10, we obtain Proposition 8.1 in the case when the exponent m of G is not 7.

8.2 when m is 7

Now we prove Proposition 8.1 in case when m is 7; that is when $G = (\mathbb{Z}/7\mathbb{Z})^r$ with r being a positive integer. In this subsection, we shall assume that m is 7.

Lemma 8.11. *Let $L \in \mathcal{L}(G)$. Then there exists a splitting (H, f) of G by $\mathbb{Z}/7\mathbb{Z}$ such that L has a presentation with respect to (H, f) and $L \neq L(H, f, H, II)$.*

Lemma 8.12. *Let $L \in \mathcal{L}(G)$. Let (H, f) be a splitting of G by $\mathbb{Z}/7\mathbb{Z}$ as in Lemma 8.11. Then for any nonzero $x \in G$ with $x \notin (H, [2, 5]_7)$, the cardinality of $R(x, L)$ is at least $\frac{n}{49}$.*

Proof. When $L \neq (H, [2, 3]_7)$, then for some proper subgroup K of H we have $(H \setminus K, [3, 4]_7) \subset L$. In this case Lemma follows using the arguments similar to those used in the proof of Lemma 8.9. Now we prove the lemma, when $L = (H, [2, 3]_7)$. Let x be a non zero element in G with $x = (x_1, i)$ with $i \notin [2, 5]_7$; that is $i \in [-1, 1]_7$. The proof is divided into two sub-cases, when $i = 0$ and when $i \neq 0$. When $i \neq 0$ we can write i either as a sum or difference of two distinct elements in $[2, 3]_7$. In this case, the lemma follows using the arguments similar to those used in proving Lemma 8.9. To prove the lemma when $i = 0$, we observe that since $x \neq 0$, it follows that $x_1 \neq 0$. Therefore there exist a subgroup K of H such that $x_1 \notin H'$ and $\mathrm{card}(H')$ is at least $\frac{n}{49}$. Therefore the sets H' and $H' + x_1$ are disjoint. Given any $z \in (H' + x_1, \{2\}_7)$ there exist a unique $y \in (H', \{2\}_7)$ such that $x = z - y$. Hence the lemma follows. □

Using Lemma 8.12, we obtain that Lemma 8.10 is true when m is 7.

9 Proof of Theorem 1.7

Using Theorem 3.5 and the simple facts that $\binom{k_2}{k_1} \leq 2^{k_2}$, we verify the following fact.

Lemma 9.1. *Let H be a finite abelian group of order n and exponent m. Let $a(H)$ be as defined in* (5)*. Then we have*

$$a(H) \leq n^{c\omega(m)n^{2/3}\log^{1/3} n}, \tag{35}$$

where c is an absolute constant.

In proving the above lemma, we also use the fact that $\omega(n) = \omega(m)$. Combining Theorem 1.8 and Lemma 9.1, we obtain Theorem 1.7.

10 Concluding remarks

The results of this paper make use of Proposition 2.2, which was proved by Ben Green and Imre Ruzsa in [5]. When there is a prime divisor of the exponent of G which is less than 1000, the arguments of Green and Ruzsa depends on highly tedious calculations which are done with the aid of computer. These calculations are not particularly tedious when the smallest prime divisor of m is sufficiently large. Ben Green has remarked to us that it would be highly desirable to obtain a different proof of this particular result of theirs.

The upper bound for $a(H)$ given by Lemma 9.1 does not appear to be best possible. Any improvement will improve the result of Theorem 1.7. For any finite abelian group H of order n, one can show that $a(H)$ is of the same order as the number of subgroups of H. Therefore when $H = (\mathbb{Z}/7\mathbb{Z})^r$, we obtain that

$$a(H) \geq 2^{c \log^2 n}, \tag{36}$$

where $c > 0$ is an absolute constant and $n = 7^r$ is the order of H. Using Theorem 3.5, one may also notice that the main contribution in the right hand side of (5) comes from those terms with k_2 close to $2k_1$.

Let $t \geq 2$ be a positive integer. We say that $A \subset G$ is t-free, if there is no solution of the equation $x_1 + x_2 + \ldots + x_t - y = 0$ with $x_i's$ and $y \in A$. We say that G is of type $(t+1, 1)$ if all the divisors of the exponent m of G are congruent to 1 modulo $t+1$. We write $\nu_t(G)$ to denote the number $\frac{\left[\frac{m-2}{t+1}\right]+1}{m} n$. When G is of type $(t+1, 1)$, a conjecture of Hamidoune and Plagne [6] states that the maximum possible cardinality $\mu_t(G)$ of t-free set in G is equal to $\nu_t(G)$. Using the arguments similar to those used in the proof of Lemma 8.4, it follows that the number of t-free subsets in any finite abelian group G of type $(t+1, 1)$ is atleast

$$a(t, H) 2^{\nu_t(G)},$$

where H is a supplement of a copy of $\mathbb{Z}/m\mathbb{Z}$ in G.

References

[1] R. Balasubramanian and Gyan Prakash. Asymptotic formula for sum-free sets in finite abelian groups. *Acta Arithmetica*, 127(2):115–124, 2007.

[2] P.H. Diananda and H.P. Yap. Maximal sum-free sets of elements of finite abelian groups. *Proc. Japan Acad*, 45:1–5, 1969.

[3] Ben Green. Counting sets with small sumset, and the clique number of random Cayley graphs. *Combinatorica*, 25(3):307–326, 2005.

[4] Ben Green. A Szemerédi-type regularity lemma in abelian groups with applications. *GAFA*, 15(2):340–376, 2005.

[5] Ben Green and Imre Ruzsa. Sum-free sets in abelian groups. *Israel J. Math*, 147:157–189, 2005.

[6] Yahya ould Hamidoune and Alain Plagne. A new critical pair theorem applied to sum-free sets in abelian groups. *Comment. Math. Helv.*, 79:183–207, 2004.

[7] Gyan Prakash. Number of sets with small sumset, and the clique number of random Cayley graph. http://arxiv.org/abs/0711.0081.

[8] A. H. Rhemtulla and A. P. Street. Maximal sum-free sets in elementary abelian p-groups. *Canad. Math. Bull.*, pages 73–80, 1971.

Institute of Mathematical Sciences,
C.I.T. Campus, Tharamani,
Chennai - 600113, India.
e-mail: balu@imsc.res.in
gyan.jp@gmail.com

Harish-Chandra Research Institute,
Chhatnag Road, Jhunsi,
Allahabad - 211 019, India.
e-mail: suri@hri.res.in